The Application Privacy, Protection, and Security (APPS) Act of 2013 (Discussion Draft)

Section-by-Section Background

SEC. 1 SHORT TITLE

The Application Privacy, Protection, and Security Act of 2013 or the APPS Act.

SEC. 2 TRANSPARENCY, USER CONTROL, AND SECURITY

The APPS Act would require that app developers maintain privacy policies, obtain consent from consumers before collecting data, and securely maintain the data that they collect.

Subsection (a) Consent

Before collecting personal data from a consumer, a developer must notify the consumer of its terms for collecting, using, sharing, storing personal data, and obtain the consumer's consent. The Federal Trade Commission would also promulgate regulations to specify the format, manner, and timing of this notice.

These terms must also disclose certain types of data-collection practices. These include the categories of personal data and purposes of its use, as well as the categories of third parties that use the personal data after it is initially collected by the developer.

Additional, developers would maintain a data-retention policy that notifies the user how long data is stored, and how to delete or opt out of data collection.

Subsection (b) Withdrawal of Consent

For consumers that no longer want to use the app, the developer would provide a mechanism for consumers to signal this intent, and to empower consumers to decide the fate of the data that has already been collected. At the consumer's election, the developer would either delete any personal data collected to the extent practicable, or cease collecting data altogether. The developer would comply with the consumer's request within a reasonable period of time.

Subsection (c) Security of personal data and de-identified data

The APPS Act would require that developers prevent unauthorized access to a user's data through reasonable and appropriate security measures. This provision would address sub-standard data storage practices by promoting responsible data storage.

Subsection (d) Exception

The APPS Act does not displace requirements for developers to disclose or preserve data under federal or state law.

SEC. 3. APPLICATION AND ENFORCEMENT

The APPS Act would be enforced through either the Federal Trade Commission under section 18(a)(1)(B) of the Federal Trade Commission Act prohibiting unfair or deceptive acts or practices, or by a state's attorney general through a federal civil action. A state could not file a civil action if a federal action is already pending.

SEC. 4. REGULATIONS

The FTC would promulgate regulations required by the Act within one year of its enactment.

SEC. 5. SAFE HARBOR

The APPS Act contains a safe harbor for companies that comply with the enforceable code of conduct agreed upon through the NTIA's multi-stakeholder process. This approach give developers flexibility in how they display their privacy policies and interact with consumers, and avoids a heavy-handed legislative approach.

SEC. 6. RELATIONSHIP TO STATE LAW

The APPS Act supersedes state law only to the extent that it provides a higher level of transparency, user control, or security of personal and de-identified data than the state.

SEC. 7. DEFINITIONS

Key definitions include "de-identified data," "personal data," "mobile application," and "mobile device."
The term "de-identified data" means data that cannot identify individuals.

The FTC will promulgate a rule to define the term "personal data," but it will not include de-identified data.

A "mobile application" is a software program that the user directly interacts with that runs on a mobile device's operating system

A "mobile device" is a smartphone, tablet computer, or similar portable computing device that transmits data over a wireless connection.

SEC. 8. EFFECTIVE DATE

The APPS Act is effective 30 days after the FTC promulgates regulations under section 4.